

Estudo Técnico Preliminar 25/2024

1. Informações Básicas

Número do processo: 71000.009328/2024-15

2. Descrição da necessidade

Apresentação A Subsecretaria de Tecnologia da Informação (STI) é a unidade responsável por desenvolver, aperfeiçoar, manter e dar suporte aos sistemas informatizados e aos bancos de dados do Ministério do Desenvolvimento e Assistência Social, Família e Combate à Fome (MDS) e do Ministério do Esporte (MESP), em acordo com o Ofício nº 232/2023/MESP/SE/CGGA (SEI 14848608) e Portaria nº 43/2023 (SEI 14849008), administrando os recursos de informação e informática dos dois órgãos. Nesse aspecto, a STI, por meio da CGI vem promovendo ações de melhoria na infraestrutura computacional do MDS e MESP, visando o melhor aproveitamento de hardware, software, serviços de rede e utilização de novas tecnologias, contando com a infraestrutura já disponível e em utilização, com ativos de rede, balanceamento de carga, segurança de rede, infraestrutura de servidores de rede e etc. A modernização, sustentação e manutenção desta infraestrutura, tanto em nível de hardware quanto softwares, garante a robustez e a estabilidade dos serviços de Tecnologia da Informação dos Ministérios. Com o intuito de manter o provimento da garantia de autenticidade, confidencialidade, integridade e não repúdio às informações eletrônicas relacionados aos serviços de Tecnologia da Informação que são prestados e/ou consumidos no âmbito do Ministério, bem como garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica conforme Medida Provisória nº 2.200-2, de 24 de Agosto de 2001, pretende-se com este projeto a substituição a continuidade da prestação de serviços que eram providos por meio do Contrato Administrativo nº 42/2020, cujo objeto era a prestação serviços de Certificação Digital segundo as normas da ICP-Brasil (Infraestrutura de Chaves Públicas Brasileiras), para fornecimento, emissão, gerenciamento e serviço de registro de certificados digitais. Necessidades: Certificados digitais para pessoa física Certificados digitais para pessoa jurídica Certificados digitais para serviços disponibilizados pelo MDS Certificados digitais para domínios ssl gerenciados pelo MDS
Motivação/Justificativa No que tange aos serviços de tecnologia da informação que são consumidos no âmbito do MDS, destacam-se alguns dos Sistemas Estruturantes da Administração Pública Federal, que necessitam da utilização de certificados digitais para o seu acesso e efetiva utilização/operacionalização, tais como: SIAPE, SIGEPE, COMPRASNET, SIAPENET, SCDP, SIASGNET, PJE e SICONV, justificando-se assim, a necessidade contínua da prestação deste tipo de serviço. Corroborando ainda, para esse entendimento, o fato de que os certificados digitais, do tipo pessoa física, são pessoais e intransferíveis, e haja vista a rotatividade existente no quadro do ministério, em especial nos gabinetes devido a natureza da instituição pública, faz-se necessário que o serviço de emissão esteja disponível.

Tendo em vista que alguns serviços do Ministério necessitam utilizar certificado digital para a escrituração fiscal digital no CNPJ do Ministério, também há a necessidade de adquirir um pequeno número de certificados digitais para Pessoa Jurídica. Essa necessidade é evidenciada, entre outros, nos processos de reembolso 71000.074627/2023-40 e 71000.076204/2023-64.

Com relação aos serviços de tecnologia da informação que são disponibilizados pelo Ministério, tais como portais web, correio eletrônico, sistemas de informações, VPN, painéis e sistemas de *business intelligence* a *web services*, busca-se com a utilização de certificados digitais garantir camadas de segurança como autenticidade, confidencialidade e integridade.

Diante do exposto e tendo em vista a preocupação ligada à segurança das informações institucionais, faz-se necessária a realização de uma análise para uma possível contratação de Pessoa Jurídica especializada para emissão de Certificados Digitais, permitindo ao Ministério assegurar a integridade das comunicações e transações eletrônicas, a confidencialidade das informações transmitidas e a simplificação dos processos administrativos que requeiram documentos oficiais assinados.

Por fim, em acordo com o Ofício nº 232/2023/MESP/SE/CGGA (SEI 14848608) e Portaria nº 43/2023 (SEI 14849008), o Ministério do Esporte utiliza os contratos referentes à Tecnologia da Informação geridos pelo MDS, desta forma a demanda a ser levantada nesse ETP deve incluir ambos os Ministérios.

Desta forma, esse ETP tem por objetivo a contratação de serviços de emissão de Certificados Digitais tipo A1 e A3, para Pessoa Física, Jurídica, Domínios e Serviços, dentro das especificações e normas do ICP-Brasil, com fornecimento parcelado, para atender a demanda do MDS e do MESP.

3. Área requisitante

Área Requisitante	Responsável
Subsecretaria de Tecnologia da Informação - SE/STI /CGINFRA	Silvino César Silveira

4. Necessidades de Negócio

Planejamento Estratégico Institucional – PEI 2023/2026 -

Necessidades de Infraestrutura de TI - NITI

NITI14A - Manter a infraestrutura de TIC compatível e aderente com as ações de transformação e sustentação digital do MDS.

NITI14B - Manter os recursos de TI compatíveis e aderentes as atividades laborais desenvolvidas pelas áreas do MDS.

NECESSIDADE DE TI - NSTI05 - Infraestrutura

Serviços associados ao conjunto de componentes técnicos, hardware, software, bancos de dados implantados, procedimentos e documentação técnica usados para disponibilizar informações, incluindo serviços de segurança digital (controle lógico e biométrico), **certificação digital**, operação e suporte técnico, backup.

Atualmente os certificados digitais são necessários para a continuidade da operação normal dos órgãos públicos em diversos níveis momentos diferentes, por exemplo:

Para a identificação de uma autoridade em um ambiente computacional;

Para a assinatura de documentos públicos em sistemas com, por exemplo, o SEI;

Para o envio de informações operacionais entre órgãos públicos de forma segura;

Para a escrituração de documentos fiscais no CNPJ do órgão ou secretaria;

Para a manutenção de serviços públicos na internet, utilizando o protocolo HTTPS ou similar;

Para identificação e tráfego encriptado de dados entre sistemas de TI de órgãos distintos.

São **Requisitos de Negócios** para o MDS:

Garantir os requisitos de segurança da informação para os sistemas e usuários do Ministério;

Garantir a autenticidade dos documentos tramitados por servidores em cargos estratégicos do Ministério;

Garantir o atendimento à legislação vigente e ser credenciada pela Infraestrutura de Chaves Públicas Brasileira – ICPBrasil;

Garantir suporte técnico adequado para os usuários do Ministério;

A solução deverá ser implementada, preferencialmente, de forma remota.

5. Necessidades Tecnológicas

A emissão dos certificados deverá ser feita em todas as instalações do Ministério, em horário comercial, preferencialmente online, de forma planejada e sempre que solicitado.

Deverá seguir o seguinte fluxo de solicitação:

A solicitação de certificado digital será feita pelo servidor mediante requerimento eletrônico contendo os dados do servidor.

Deverá seguir o seguinte fluxo de aprovação:

A aprovação da solicitação de certificado digital é concedida pelo autorizador designado pelo Ministério. Para realizar o procedimento o autorizador acessará o sistema do fornecedor, selecionará em uma lista a solicitação do servidor e realizará a aprovação;

Ao aprovador, só será permitido realizar a ação se ele cumprir, no momento, os requisitos para aprovação de certificados conforme preconizado pelo Ministério.

Após a aprovação, o fornecedor de certificados envia para o e-mail institucional do servidor solicitante as orientações para baixar e instalar o certificado digital.

Deverá seguir o seguinte fluxo de instalação:

A instalação do certificado digital será feita pelo próprio servidor. Ele deverá seguir as orientações encaminhadas por e-mail após a aprovação da solicitação de certificado digital.

Para a instalação, o servidor deverá realizar o download do aplicativo em sua máquina local.

Deverá seguir o seguinte fluxo para suporte técnico:

Acionar os canais de comunicação do atendimento técnico da STI.

O atendimento técnico da STI deverá abrir um chamado com o fornecedor de certificados digitais, quando for o caso.

O fornecedor de certificados deverá obedecer ao seguinte acordo de nível de serviço:

Fornecimento de certificado digital: Em até 48 horas após aprovação do autorizador designado pelo Ministério;

Acionamentos associados a problemas ou dúvidas que não afetam a operação do sistema (habilitação de usuários, etc): O tratamento de acionamento será realizado em horário comercial, por meio de solicitação de serviço;

Acionamentos associados a problemas que criam restrições à operação do sistema, porém não afetam a sua funcionalidade: O tratamento de acionamento será realizado em horário comercial, por meio de solicitação de serviço;

Acionamentos associados a eventos que não fazem parte da operação normal de um serviço e que causem ou venham causar uma interrupção ou redução da qualidade de serviço (indisponibilidade, intermitência, etc): O tratamento de acionamento de severidade alta é realizado em período ininterrupto, durante 24 (vinte e quatro) horas por dia e 7 (sete) dias por semana. A Central de Serviços classificará este chamado em registro de incidente.

ABNT NBR ISO/IEC 27001

define um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI).

define os principais requisitos para segurança da informação:

Confidencialidade: Propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados;

Integridade: propriedade de salvaguarda da exatidão e completeza de ativos;

Autenticação: Garantia de que a entidade se comunicando é aquela que ela afirma ser;

Irretratabilidade: Oferece proteção contra negação, por parte de uma das entidades envolvidas em uma comunicação, de ter participado de toda ou parte de comunicação;

Disponibilidade: Propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada.

ICP-Brasil

Por força da legislação atual e para garantir a validade jurídica aos atos praticados com seu uso, os certificados deverão ser emitidos seguindo regras do Comitê Gestor da ICP-Brasil.

O certificado deve ser emitido por Autoridade Certificadora credenciada pela Infraestrutura de Chaves Públicas Brasileira – ICPBrasil.

São **Requisitos Tecnológicos** para o MDS:

A solução deve seguir padrões típicos de mercado;

A solução deve ser de fácil instalação e configuração;

A solução deve ser compatível com os sistemas e soluções presentes no Ministério;

A solução deve ter garantia e suporte pelo período de 36 meses;

A solução deve ser individual para cada servidor em cargos estratégicos do Ministério;

A solução deve garantir a proteção adequada para os níveis estratégicos do Ministério.

6. Demais requisitos necessários e suficientes à escolha da solução de TIC

Requisitos de Treinamento e Transferência de Conhecimento:

Deverá ser disponibilizado manual para os usuários e administradores em formato digital.

Requisitos de Garantia e Suporte Técnico:

Todos os itens adquiridos deverão possuir garantia e suporte técnico inclusos;

Modo de atendimento poderá ser presencial ou remoto.

Requisitos de Segurança da Informação:

A Contratada e todos os seus funcionários envolvidos na prestação dos serviços deverão atender integralmente às diretrizes da Política de Segurança da Informação e Comunicações do MDS;

A Contratada deverá garantir a segurança das informações do Ministério e se comprometer a não divulgar ou fornecer a terceiros quaisquer dados e informações que tenha recebido deste Ministério no curso da prestação dos serviços, a menos que autorizado formalmente;

Todo e qualquer tipo de acesso remoto necessário ao diagnóstico de falhas ou manutenção de equipamentos deverá ser previamente autorizado pelo MDS.

Requisitos sociais, ambientais e culturais:

A Contratada deverá atender, no que couber, os critérios de sustentabilidade ambiental definidos em legislação específica;

Os equipamentos substituídos que não estiverem em condições de uso serão encaminhados para desfazimento conforme política vigente;

A Contratada deverá fazer a destinação correta de caixas e embalagens utilizados no transporte de peças, componentes e equipamentos.

Requisitos legais:

Lei Federal nº 14.133/2021 - Estabelece normas gerais de licitação e contratação para as Administrações Públicas diretas, autárquicas e fundacionais da União, dos Estados, do Distrito Federal e dos Municípios;

Lei nº 13.709/2019 - Dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Decreto nº 7.174/2010 - Regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal, direta ou indireta, pelas fundações instituídas ou mantidas pelo Poder Público e pelas demais organizações sob o controle direto ou indireto da União;

Decreto nº 7.579/2011 - Dispõe sobre o Sistema de Administração dos Recursos de Tecnologia da Informação - SISIP, do Poder Executivo federal;

Medida Provisória nº 2.200-2/2001 - Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências.

Instrução Normativa 01/2010 SLTI/MP - Dispõe sobre os critérios de sustentabilidade ambiental na aquisição de bens, contratação de serviços ou obras pela Administração Pública Federal direta, autárquica e fundacional e dá outras providências;

Instrução Normativa 01/2019 SGD/MP - Dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação (SISIP) do Poder Executivo Federal;

Instrução Normativa 65/2021 SEGES/ME - Dispõe sobre o procedimento administrativo para a realização de pesquisa de preços para aquisição de bens e contratação de serviços em geral, no âmbito da administração pública federal direta, autárquica e fundacional.

Instrução Normativa 94/2022 SGD/ME - Dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISIP do Poder Executivo Federal.

Instrução Normativa 06/2023 SGD/MGI - Regulamenta os requisitos e procedimentos para aprovação de contratações ou de formação de atas de registro de preços, a serem efetuados por órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISIP do Poder Executivo federal, relativos a bens e serviços de tecnologia da informação e comunicação - TIC.

Portaria 6.432/2018 MPDG/STI - Dispõe sobre a aplicação do Índice de Custos de Tecnologia da Informação no âmbito da Administração Pública Federal direta, autárquica e fundacional e dá outras providências;

Política de Segurança da Informação e Comunicações (POSIC) do MDS;

PDTI 2023-2027 - Plano Diretor de Tecnologia da Informação (PDTI) - portaria MDS nº 963

7. Estimativa da demanda - quantidade de bens e serviços

Certificados para Pessoa Física

Demanda MDS

O Decreto nº 11.392/2023, de 20 de janeiro de 2023, "Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança do Ministério do Desenvolvimento e Assistência Social, Família e Combate à Fome, e transforma e remaneja cargos em comissão e funções de confiança".

O Decreto nº 11.634/2023, de 14 de Agosto de 2023, "Altera o Decreto nº 11.392, de 20 de janeiro de 2023, que aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança do Ministério do Desenvolvimento e Assistência Social, Família e Combate à Fome, e remaneja e transforma cargos em comissão e funções de confiança".

Este último, em seu Anexo II, apresenta o quadro resumo dos cargos em comissão, das funções de confiança e das funções gratificadas do MDS, cujo quantitativo de cargos para os níveis de Coordenador (ou equivalente) ou superior é apresentado na Tabela 7-A:

Tabela 7-A: Quantitativo de cargos MDS

CÓDIGO	Quantidade
CCE 1.18	1
CCE 1.17	8
CCE 1.15	31
CCE 1.14	1
CCE 1.13	57
CCE 1.11	1
CCE 1.10	62
CCE 1.09	1
CCE 1.07	31
CCE 1.05	5
CCE 2.15	2
CCE 2.13	5
CCE 2.10	5
CCE 2.07	5

CCE 3.15	2
CCE 3.13	12
CCE 3.10	17
CCE 3.09	2
CCE 3.08	1
CCE 3.07	26
CCE 3.05	4
FCE 1.15	5
FCE 1.13	57
FCE 1.10	80
FCE 1.07	40
FCE 1.05	2
FCE 2.13	1
FCE 2.10	1
FCE 3.15	1
FCE 3.13	11
FCE 3.10	25
FCE 3.08	2
FCE 3.07	29
FCE 3.06	1

FCE 3.05	1
FCE 3.04	1
FCE 3.02	21
FCE 3.01	4
FCE 4.05	1
FCE 4.04	1
FCE 4.03	35
TOTAL DE CARGOS NO MDS	598

Demanda MESP

O Decreto 11343 / 2023 - Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança do Ministério do Esporte e remaneja cargos em comissão e funções de confiança.

O Decreto 11450 / 2023 - Altera o Decreto nº 11.343, de 1º de janeiro de 2023, que aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança do Ministério do Esporte.

Este último, em seu Anexo II, apresenta o quadro resumo dos cargos em comissão, das funções de confiança e das funções gratificadas do MESP, cujo quantitativo de cargos para os níveis de Coordenador (ou equivalente) ou superior é apresentado na Tabela 7-B:

Tabela 7-B: Quantitativo de cargos MESP

CÓDIGO	Quantidade
CCE 1.18	1
CCE 1.17	5
CCE 1.15	15
CCE 1.14	2
CCE 1.13	26
CCE 1.10	8
CCE 1.07	7

CCE 2.15	2
CCE 2.13	3
CCE 2.10	12
CCE 2.07	6
CCE 2.05	1
CCE 3.13	1
FCE 1.15	3
FCE 1.13	16
FCE 1.10	8
FCE 1.07	7
FCE 2.13	7
FCE 2.10	12
FCE 2.07	31
FCE 2.05	5
TOTAL DE CARGOS NO MESP	178

Demanda de certificados Pessoa Física

Conforme as Tabelas 7-A e 7-B, os Ministérios atualmente possuem 776 cargos considerados estratégicos (598 no MDS e 178 no MESP), sendo que cerca de 20% (1/5) destes cargos utilizam Certificados Digitais com Token, valor menor que o previsto no contrato anterior (SEI 71000.011752/2020-04), que era 1/3 dos certificados usarem tokens.

Assim, opta-se por atualizar esse critério para 1/5 (20% dos certificados usarão Tokens) e, considerando os eventuais substitutos e a rotatividade de cargos característica do poder executivo, opta-se também por reduzir o quantitativo adicional (margem de segurança) utilizado para 50% do total.

A Tabela 7-C sumariza as quantidades de certificados digitais para pessoa física, dos tipos A1 ou A3 compatíveis com ICP-Brasil, necessárias aos Ministérios:

Tabela 7-C - Quantidade de certificados para pessoa física

	com Token	sem Token	Total
Certificados PF	156	620	776
Margem (50%)	78	310	388
Total	234	930	1164

Esse quantitativo atende aos seguintes requisitos da contratação:

Requisito de negócio 2: Garantir a autenticidade dos documentos tramitados por servidores em cargos estratégicos do Ministério;

Requisito tecnológico 5: A solução deve ser individual para cada servidor em cargos estratégicos do Ministério.

Certificados para Pessoa Jurídica

A partir de outubro de 2023 passou a ser obrigatório às Unidades Gestoras do Governo do preenchimento da Escrituração Fiscal Digital de Retenções e Outras Informações Fiscais (EFD-Reinf), instituída pela Instrução Normativa RFB nº 1701, de 17 de março de 2017. O acesso ao sistema ocorre por intermédio da Autenticação Gov.br utilizando um certificado digital de pessoa física ou jurídica, dos tipos A1 ou A3 compatíveis com ICP-Brasil. O certificado deve ser emitido por Autoridade Certificadora credenciada pela Infraestrutura de Chaves Públicas Brasileira – ICPBrasil, que deve pertencer à série “A”.

Essa escrituração fiscal digital - EFD do r. CNPJ junto a Secretaria Especial da Receita Federal do Brasil, é realizada por meio do acesso ao Centro Virtual de Atendimento - ECAC, na forma prevista no Manual de orientação do usuário Versão 2.1.1.1 do Sistema Público de Escrituração Digital - Sped, EFD-Reinf, e se realiza SOMENTE com certificados digitais.

É necessário a emissão de tais certificados para os seguintes setores do MDS:

Tabela 7-D - Setores com escrituração fiscal MDS

	Cód	Secretarias	CNPJ
1	550002	SETORIAL DE ORÇAMENTO E FINANÇAS	5756246000101
2	550003	DIREÇÃO NACIONAL DE PROJETOS-DNP - MC	5526783000165
3	550004	SETORIAL DE CONTABILIDADE E CUSTOS	5526783000165
4	550005	COORDENACAO GERAL DE LICITACOES E CONTRATOS.	5756246000454
5	550006	COORDENACAO-GERAL DE GESTAO DE PESSOAS/MDS	5756246000373
6	550007	SECRETARIA NACIONAL DE RENDA DA CIDADANIA	5526783000165
7	550008	SECRETARIA NAC. DE SEGUR. ALIMENTAR E NUTRIC.	5526783000408
8	550009	DPTO. APOIO E ACOLHIM. AT. EM ÁLCOOL E DROGAS	5526783000165

9	550010	SECRET. AVAL., GESTAO DA INFORM. E CAD. UNICO	5526783000165
10	550011	SECRETARIA NACIONAL DE ASSISTENCIA SOCIAL.	1002940000182
11	550013	PROJETO DE OPERACIONALIZ. DOS PROGRAMAS SESAN	5526783000246
12	550015	PROJETO DE OPERACION. DOS PROGRAMAS DA SNAS	1002940000182
13	550017	II PROJETO DE APOIO AO PBF E AO CNDS	5526783000165
14	550018	SECRETARIA DE INCLUSÃO SOCIOECONÔMICA	5526783000165
15	550019	II PROJETO DE APOIO AO PBF E CNDS - DOLAR	5526783000165
16	550020	PROJ. DE OPERAC. DOS PROGRAMAS SESAN/BNB	5526783000165
17	550023	SECRETARIA NACIONAL DE CUIDADOS E FAMÍLIA	5526783000165
18	550025	SAA/SE/MC - CONDOMINIO BLOCO A	5756246000454

Além disso, é necessário a emissão de tais certificados para os seguintes setores do MESP:

Tabela 7-E - Setores com escrituração fiscal MESP

	Cód	Secretarias	CNPJ
1		ABCD - Associação Brasileira de Controle de Dopagem	2961362000689
2		POB - Parque Olímpico da Barra	2961362000174
3		Secretaria Executiva	2973091000177

Demanda de certificados para Pessoa Jurídica

Conforme as Tabela 7-D e 7-E, os Ministérios atualmente possuem 21 setores que necessitam executar o processo de escrituração fiscal (18 do MDS e 3 do MESP). No entanto, deve-se considerar a necessidade de ter dois responsáveis em cada setor, e também uma margem de 30% do total para atender novas secretarias, os eventuais substitutos e a rotatividade de cargos característica do poder executivo.

A Tabela 7-F sumariza as quantidades de certificados digitais para pessoa jurídica, dos tipos A1 ou A3 compatíveis com ICP-Brasil, necessárias aos Ministérios:

Tabela 7-F - Quantidade de certificados para Pessoa Jurídica

	Secretarias	Quantidade Certificados
--	-------------	-------------------------

MDS	18	36
MESP	3	6
Subtotal:	21	42
Margem (30%):	6	12
Total de Certificados PJ:		54

Certificados para Domínios e Serviços do MDS

Os certificados digitais para servidor são utilizados tanto para prover o acesso seguro de usuários aos ambientes web dos Ministérios (**certificados de domínio**), quanto para prover comunicação segura entre os servidores de aplicação do MDS e do MDES (**certificados de serviços**) e outros entes públicos como, por exemplo, a Receita Federal, Caixa Econômica Federal, Serpro ou qualquer outro serviço que necessite de comunicação segura.

Certificados de Domínio

Os certificados de domínio são utilizados para garantir a autenticidade das páginas web sob a responsabilidade e gestão dos MDS e do MESP, garantindo ao usuário a certeza de estar trafegando por uma ambiente oficial do ministério. Essa garantia (representada pelo cadeado fechado no acesso via browser) é essencial para a correta prestação dos serviços web públicos de ambos os ministérios.

Todos os certificados em utilização atualmente são certificados A1, modelo "Wildcard", com validade de 12 meses.

Atualmente existem 5 (cinco) domínios administrados pela SGI:

*.mds.gov.br,

*.esporte.gov.br,

*.cidadania.gov.br,

*.abcd.gov.br e

*.desenvolvimentosocial.gov.br

Certificados de Serviço

Os certificados de serviço do tipo SSL são utilizados para assinaturas que precisam tramitar com outros órgãos. Ressalta-se que esses certificados são requisito para a integração dos sistemas dos Ministérios com outros sistemas governamentais como, por exemplo: SIAFI, SISGRU, SIGTV e SIGTR.

Para a maioria dos sistemas a serem integrados há a exigência de **certificados A1 ou A3 sem token, emitidos dentro da cadeia de autoridade da ICP-Brasil**.

Esses sistemas possuem dois ambientes (homologação e produção) e ambos necessitam de certificado para a correta administração do serviço. Nesse sentido, são necessários dois certificados para cada serviço que os utilizam: um para o ambiente de HOMOLOGAÇÃO e outro para ambiente de PRODUÇÃO.

Atualmente existem 5 (cinco) sistemas em produção e/ou desenvolvimento que utilizam estes certificados. Por exemplo: SEI, SIGTR, SIAFI, AlimentaBrasil e Vejae.

Demanda de certificados para Domínios e Serviços

Tabela 7-G - Quantidade de certificados de domínio e serviço

	Wildcard	Produção	Homologação
Atual	5	5	5
Margem (20%)	-	1	1
Crescimento anual	1	2	2
Totais 2024	6	8	8
Totais 2025	7	10	10
Totais 2026	8	12	12

8. Levantamento de soluções

Do uso de certificados digitais

O certificado digital é uma solução consolidada para garantir os requisitos de segurança em um ambiente corporativo, no qual diversos níveis de acesso devem ser controlados e protegidos. **Esse tipo de tecnologia utiliza criptografia de chaves públicas para proteger a confidencialidade, a integridade, a autenticação e a irretratabilidade das comunicações e dos usuários.**

Quando a criptografia de chave pública é utilizada, as chaves públicas de usuários ou sistemas podem estar assinadas digitalmente por uma autoridade certificadora (*Certification Authority* - CA) confiável, de modo que a utilização ou publicação falsa dessas chaves pode ser evitada. As chaves públicas assinadas digitalmente por uma autoridade certificadora confiável constituem, assim, os certificados digitais. A autoridade certificadora, os usuários, os sistemas e seus certificados digitais fazem parte de um modelo de confiança essencial em um ambiente cooperativo, necessário para a identificação, autenticação e acesso seguro aos sistemas críticos.

Os certificados digitais são, normalmente, criados pelas autoridades certificadoras, que têm a função de criar, manter e controlar todos os certificados por elas emitidos, incluindo a invalidação de certificados comprometidos ou expirados. A manutenção da CA envolve a segurança de sua própria chave privada que, caso seja descoberta ou roubada, comprometerá todo o sistema.

De acordo com o art. 10, da MP nº 2.200-2, os documentos eletrônicos assinados digitalmente com o uso de certificados emitidos no âmbito da ICP-Brasil têm a mesma validade jurídica que os documentos em papel com assinaturas manuscritas. Importante frisar que os documentos eletrônicos assinados digitalmente por meio de certificados emitidos fora do âmbito da ICP-Brasil também têm validade jurídica, mas esta dependerá da aceitação de ambas as partes, emitente e destinatário, conforme determina a redação do § 2º do art. 10 da MP nº 2.200-2.

O certificado digital da ICP-Brasil, além de personificar o cidadão na rede mundial de computadores, garante, por força da legislação atual, validade jurídica aos atos praticados com seu uso. A certificação digital é uma ferramenta que permite que

aplicações, como comércio eletrônico, assinatura de contratos, operações bancárias, iniciativas de governo eletrônico, entre outras, sejam realizadas. São transações feitas de forma virtual, ou seja, sem a presença física do interessado, mas que demandam identificação inequívoca da pessoa que a está realizando pela Internet.

Tecnicamente, o certificado é um documento eletrônico que por meio de procedimentos lógicos e matemáticos asseguraram a integridade das informações e a autoria das transações. Esse documento eletrônico é gerado e assinado por uma terceira parte confiável, ou seja, uma Autoridade Certificadora que, seguindo regras emitidas pelo Comitê Gestor da ICP-Brasil e auditada pelo ITI, associa uma entidade (pessoa, processo, servidor) a um par de chaves criptográficas.

Considerando as possibilidades enumeradas no inciso II do art 11, temos que:

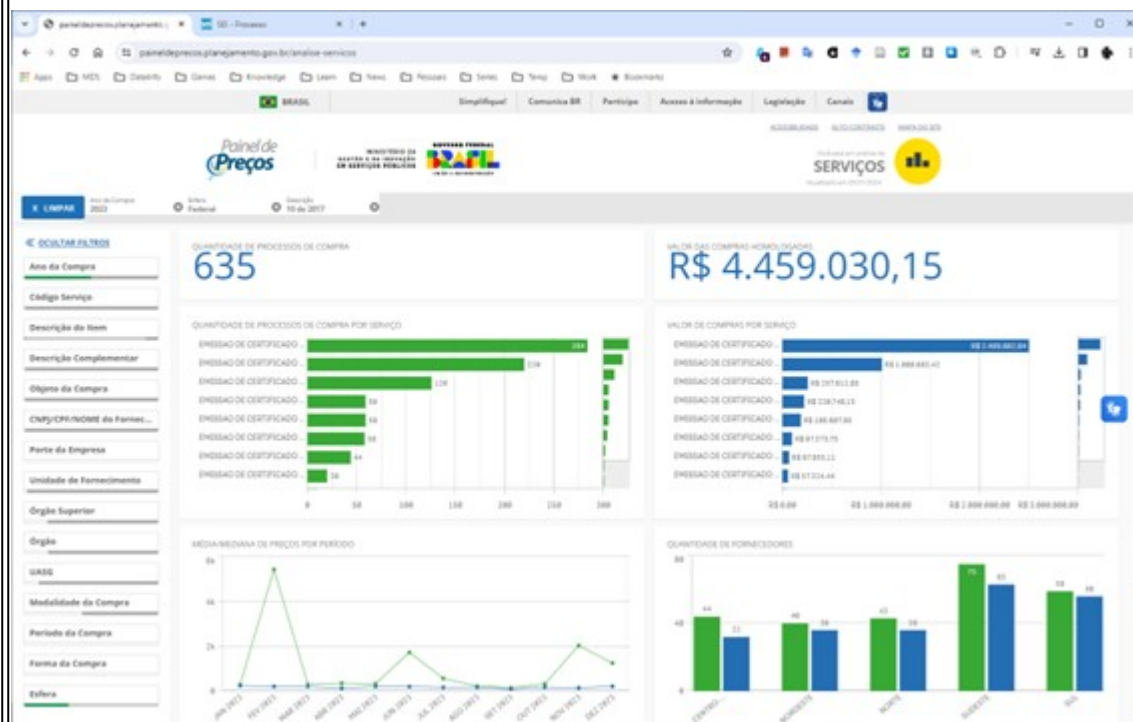


Figura 8-A - Pesquisa no Pannel de Preços

Necessidades similares em outros órgãos ou entidades da Administração Pública e as soluções adotadas

Conforme demonstrado na Figura 8-A, acima, uma pesquisa pelo termo "Certificado Digital" no Pannel de Preços (<https://paineldepresos.planejamento.gov.br/>) mostra que foram realizadas 635 aquisições similares por órgãos do governo federal no ano de 2023. Desta forma, resta claro que a solução em questão é bem conhecida e amplamente utilizada.

As alternativas do mercado

A mesma pesquisa demonstrada na Figura 8-A mostra que houveram 40 (ou mais) empresas diferentes participando das licitações em cada uma das 5 regiões do país, com 30 (ou mais) empresas homologadas nos processos.

A existência de softwares disponíveis conforme descrito na Portaria STI/MP nº 46, de 28 de setembro de 2016, e suas atualizações

Não se aplica, já que a aquisição em questão é de certificados digitais, que serão utilizados pelos softwares. Estes certificados precisam ser assinados por uma Autoridade Certificadora, seguindo regras emitidas pelo Comitê Gestor da ICP-Brasil e auditada pelo ITI.

As políticas, os modelos e os padrões de governo, a exemplo dos Padrões de Interoperabilidade de Governo Eletrônico - ePing, Modelo de Acessibilidade em Governo Eletrônico - eMag, Padrões Web em Governo Eletrônico - ePwg, padrões de Design System de governo, Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil e Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos - e-ARQ Brasil, quando aplicáveis

Conforme descrito acima, os certificados em questão deverão atender o padrões definidos na Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil.

As necessidades de adequação do ambiente do órgão ou entidade para viabilizar a execução contratual (exemplo: mobiliário, instalação elétrica, espaço adequado para prestação do serviço, etc)

Os servidores e serviços do MDS já utilizam certificados digitais, não sendo necessária novas adequações.

Os diferentes modelos de prestação do serviço

A utilização de certificados do tipo A1 ou A3, com ou sem token, e com 12 ou 36 meses de validade será tratada mais adiante na análise de soluções possíveis.

Os diferentes tipos de soluções em termos de especificação, composição ou características dos bens e serviços integrantes

A utilização de certificados do tipo A1 ou A3, com ou sem token, e com 12 ou 36 meses de validade será tratada mais adiante na análise de soluções possíveis.

A possibilidade de aquisição na forma de bens ou contratação como serviço

A aquisição de certificados na forma de serviço é amplamente aceita, como visto na pesquisa da Figura 8-A, acima.

A ampliação ou substituição da solução implantada

O crescimento natural necessário foi discutido no item 7 - Estimativa da Demanda, acima.

As diferentes métricas de prestação do serviço e de pagamento

As diferentes métricas de prestação do serviço e de pagamento serão tratadas mais adiante, na análise das soluções.

Levantamento de soluções para atendimento às necessidades dos Ministérios

Certificados para Pessoa Física

Tabela 8-A

Id	Descrição da solução
PF01	CATSER 27146 - EMISSAO DE CERTIFICADO DIGITAL A1 PARA PESSOA FISICA
	• Certificado A1, • Pessoa Física (e-CPF), • ICP-Brasil, • validade de 12 meses
PF02	CATSER 27154 - EMISSAO DE CERTIFICADO DIGITAL MOBILE PARA PESSOA FISICA
	• Certificado A3, • Pessoa Física (e-CPF), • ICP-Brasil, • em nuvem, • validade de 36 meses
PF03	CATSER 27189 - EMISSAO DE CERTIFICADO DIGITAL A3, COM TOKEN PESSOA FISICA
	• Certificado A3, • Pessoa Física (e-CPF), • ICP-Brasil, • COM token físico,

	• validade de 36 meses
PF04	CATSER 27219 - EMISSAO DE CERTIFICADO DIGITAL A3, SEM TOKEN PESSOA FISICA • Certificado A3, • Pessoa Física (e-CPF), • ICP-Brasil, • SEM token físico, • validade de 36 meses
PF05	Híbrida PF02, PF03 e PF04 • Demanda principal atendida utilizando a Solução PF02 em Nuvem • Pequeno grupo de autoridades atendido usando a Solução PF03, COM token • Renovação de certificados COM token utilizando a Solução PF04, SEM token, quando a mídia estiver em condições
Certificados para Pessoa Jurídica	
Tabela 8-B	
Id	Descrição da solução
PJ01	CATSER 27162 - EMISSAO DE CERTIFICADO DIGITAL A1 PARA PESSOA JURIDICA • Certificado A1, • Pessoa Jurídica (e-CNPJ), • ICP-Brasil, • validade de 12 meses
PJ02	CATSER 27197 - EMISSAO DE CERTIFICADO DIGITAL A3, COM TOKEN PESSOA JURIDICA • Certificado A3, • Pessoa Jurídica (e-CNPJ), • ICP-Brasil, • COM token físico, • validade de 36 meses
PJ03	CATSER 27227 - EMISSAO DE CERTIFICADO DIGITAL A3, SEM TOKEN PESSOA JURIDICA • Certificado A3, • Pessoa Jurídica (e-CNPJ), • ICP-Brasil, • SEM token físico, • validade de 36 meses
Certificados para Servidores - Serviços	
Tabela 8-C	

Id	Descrição da solução
SS01	CATSER 27170 - EMISSAO DE CERTIFICADO DIGITAL A1 PARA EQUIPAMENTO SERVIDOR
	• Certificado A1, • para equipamento servidor, • ICP-Brasil, • validade de 12 meses, • para integração com aplicações de governo, como: SEI, SIAFI, SIGTR, SISGRU, GOV.BR, etc.
SS02	CATSER 27235 - EMISSAO DE CERTIFICADO DIGITAL A3, SEM TOKEN PARA EQUIPAMENTO SERVIDOR
	• Certificado A1, • para equipamento servidor, • ICP-Brasil, • validade de 36 meses, • SEM token físico, • para integração com aplicações de governo, como: SEI, SIAFI, SIGTR, SISGRU, GOV.BR, etc.

Certificados para Servidores - Domínios

Tabela 8-D

Id	Descrição da solução
SD01	CATSER 27170 - EMISSAO DE CERTIFICADO DIGITAL A1 PARA EQUIPAMENTO SERVIDOR
	• Certificado A1, • para equipamento servidor, • ICP-Brasil, • modo wildcard (por exemplo: *.mds.gov.br, *.esporte.gov.br), • validade de 12 meses
SD02	CATSER 27235 - EMISSAO DE CERTIFICADO DIGITAL A3, SEM TOKEN PARA EQUIPAMENTO SERVIDOR
	• Certificado A1, • para equipamento servidor, • ICP-Brasil, • modo wildcard (por exemplo: *.mds.gov.br, *.esporte.gov.br), • SEM token físico, • validade de 36 meses

9. Análise comparativa de soluções

Soluções para certificados para pessoa física

Solução PF01 - EMISSÃO DE CERTIFICADO DIGITAL A1 PARA PESSOA FÍSICA

Tabela 9-A

Solução:	PF01 - EMISSÃO DE CERTIFICADO DIGITAL A1 PARA PESSOA FÍSICA
Descrição:	Essa é a solução mais antiga, os certificados são gerados e armazenados em um arquivo encriptado com acesso por senha. O usuário precisa instalar o arquivo nos ambientes onde precisar usar o certificado
Vantagens:	1. O certificado pode ser transferido para outros ambientes.
Desvantagens:	1. O arquivo pode ser facilmente copiado, ainda que precise da senha para ser descriptografado; 2. O usuário precisa saber manusear e instalar o arquivo do certificado em vários sistemas.
Análise Operacional:	Não atende
	O impacto no processo de geração e uso dos recursos de atendimento de TI é muito grande, tornando esse modelo inviável operacionalmente .

Solução PF02 - EMISSÃO DE CERTIFICADO DIGITAL MOBILE PARA PESSOA FÍSICA

Tabela 9-B

Solução:	PF02 - EMISSÃO DE CERTIFICADO DIGITAL MOBILE PARA PESSOA FÍSICA
Descrição:	A solução em Nuvem dispensa a utilização de equipamento físico, os certificados são gerados e armazenados em nuvem.
Vantagens:	1. O usuário utiliza seu próprio smartphone para assinatura de documentos; 2. O certificado pode ser transferido para outro smartphone; 3. Ganho em gestão, já que o armazenamento na nuvem permite uma melhor administração desses recursos.
Desvantagens:	1. Necessita que o usuário tenha um smartphone com acesso à Internet.
	Atende com ressalvas

Análise Operacional:	Este é o modelo mais utilizado atualmente no Ministério , tendo a melhor viabilidade operacional. No entanto, ele não é adequado para o tratamento de assinaturas de autoridades em postos mais sensíveis do Ministério.
-----------------------------	---

Solução PF03 - EMISSÃO DE CERTIFICADO DIGITAL A3, COM TOKEN PESSOA FÍSICA

Tabela 9-C

Solução:	PF03 - EMISSÃO DE CERTIFICADO DIGITAL A3, COM TOKEN PESSOA FÍSICA
Descrição:	O TOKEN é um dispositivo físico capaz de gerar e armazenar as chaves criptográficas que compõe os Certificados Digitais. Normalmente esse dispositivo é conectado aos computadores por meio da porta USB.
Vantagens:	- Solução mais tradicional, os usuários do Ministério estão acostumados a utilizar certificado digital com token; - Ganho em segurança com a utilização de dispositivo específico para o tratamento de certificados (token); - Não existe a necessidade de instalar aplicativos em smartphones.
Desvantagens:	A perda do token resulta na perda do certificado.
Análise Operacional:	Atende com ressalvas Este modelo apresenta ganho significativo de segurança, devido à utilização de um dispositivo especializado para o tratamento dos certificados. Sendo, por isso, o mais indicado para situações onde o ganho em segurança é necessário. Por exemplo, para o uso de autoridades em postos mais sensíveis no Ministério. No entanto ele tem um custo maior, não sendo adequado para atender a um grande número de usuários.

Solução PF04 - EMISSÃO DE CERTIFICADO DIGITAL A3, SEM TOKEN PESSOA FÍSICA

Tabela 9-D

Solução:	PF04 - EMISSÃO DE CERTIFICADO DIGITAL A3, SEM TOKEN PESSOA FÍSICA
Descrição:	Essa é a solução similar à solução PF01, onde os certificados são gerados e armazenados em um arquivo encriptado com acesso por senha ou diretamente em um dispositivo token já existente. O usuário precisa instalar o arquivo nos ambientes onde precisar usar o certificado.
Vantagens:	- O certificado pode ser transferido para outros ambientes; - O certificado A3 pode ser emitido com validade 36 meses, ao contrário do certificado A1;

	3. O certificado pode ser gerado em um token físico já existente (token com certificado vencido).
Desvantagens:	1. Se gerado em arquivo pode ser facilmente copiado, ainda que precise da senha para ser descriptografado; 2. Se gerado em arquivo o usuário precisa saber manusear e instalar o arquivo do certificado em vários sistemas.
Análise Operacional:	Não atende Essa solução é similar à PF01 e inviável operacionalmente pelos mesmos motivos já citados. No entanto ela pode ser utilizada para o processo de renovação dos tokens físicos já existentes, a um menor custo que o da solução PF03.

Solução PF05 - Híbrida PF02, PF03 e PF04

Tabela 9-E

Solução:	Solução PF05 - Híbrida PF02, PF03 e PF04
Descrição:	Essa solução descreve o modelo atualmente implantado no Ministério. Ela considera um misto de certificados A3 em Nuvem para a maioria dos usuários e certificados A3 em token físico para as autoridades em postos mais sensíveis, aproveitando as vantagens de cada solução.
Vantagens:	1. É a solução atualmente implantada no Ministério; 2. Solução mais tradicional, as autoridades do Ministério já estão acostumados a utilizar certificado digital com token; 3. Ganho em segurança com a utilização de dispositivo específico para o tratamento de certificados (token) em postos mais sensíveis; 4. O usuário normal já utiliza seu próprio smartphone para assinatura de documentos; 5. O certificado pode ser transferido para outro smartphone; 6. Ganho em gestão, já que o armazenamento na nuvem permite uma melhora administração desses recursos; 7. Permite o reaproveitamento das mídias físicas (token) na emissão de novo certificado.

Desvantagens:	1. A perda do token resulta na perda do certificado; 2. Necessita que o usuário tenha um smartphone com acesso à Internet.
Análise Operacional:	Atende
	Esse é o modelo em operação no Ministério, com a adição do reaproveitamento dos tokens antigos com certificados vencidos. A Solução apresenta as vantagens descritas nas soluções PF02 e PF03, com o balanceamento econômico da utilização da PF03, mais cara, apenas para os cargos mais sensíveis.

Proporções utilizadas na solução Híbrida

A Tabela 7-C acima determina a quantidade de certificados (com token e sem token) existentes;

156 certificados COM token físicos perderão a validade;

Considerando que 50% das mídias físicas em uso poderão ser reutilizadas na renovação.

Tabela 9-F

	Nuvem CATSER 27154	COM Token		Total de Certificados PF (36 meses)
		Novos CATSER 27189	Renovação CATSER 27219	
Qtd por ano	310	52	26	388
Qtd Total	930	156	78	1164

Comparação das soluções para pessoa física

Tabela 9-G

Comparação das soluções para pessoa física		Soluções				
Requisitos		PF01	PF02	PF03	PF04	PF05
Negócio	Garantir os requisitos de segurança da informação para os sistemas e usuários do Ministério	Atende	Atende	Atende	Atende	Atende
	Garantir a autenticidade dos documentos tramitados por servidores em cargos estratégicos do Ministério	Atende	Atende	Atende	Atende	Atende
	Garantir o atendimento à legislação vigente e ser credenciada pela Infraestrutura de Chaves Públicas Brasileira – ICPBrasil	Atende	Atende	Atende	Atende	Atende
	Garantir suporte técnico adequado para os usuários do Ministério	Atende	Atende	Atende	Atende	Atende

	A solução deverá ser implementada, preferencialmente, de forma remota	Atende	Atende	Atende	Atende	Atende
Tecnológico	A solução deve seguir padrões típicos de mercado	Atende	Atende	Atende	Atende	Atende
	A solução deve ser de fácil instalação e configuração	Não atende	Atende	Atende	Não atende	Atende
	A solução deve ser compatível com os sistemas e soluções presentes no Ministério	Atende	Atende	Atende	Atende	Atende
	A solução deve ter garantia e suporte pelo período de 36 meses	Atende	Atende	Atende	Atende	Atende
	A solução deve ser individual para cada servidor em cargos estratégicos do Ministério	Atende	Atende	Atende	Atende	Atende
	A solução deve garantir a proteção adequada para os níveis estratégicos do Ministério	Não atende	Não atende	Atende	Não atende	Atende
Outros	A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	sim	sim	sim	sim	sim
	A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	não se aplica	não se aplica	não se aplica	não se aplica	não se aplica
	A Solução é composta por software livre ou software público? (quando se tratar de software)	não se aplica	não se aplica	não se aplica	não se aplica	não se aplica
	A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	não se aplica	não se aplica	não se aplica	não se aplica	não se aplica
	A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	sim	sim	sim	sim	sim
	A solução faz parte do Catálogo de Soluções de TIC - SISP?	não	não	não	não	não
Resultado da Análise		Não viável	Não viável	Viável	Não viável	Viável

Soluções para certificados para pessoa jurídica

Solução PJ01 - EMISSÃO DE CERTIFICADO DIGITAL A1 PARA PESSOA JURÍDICA

Tabela 9-H

--	--

Solução:	PJ01 - EMISSÃO DE CERTIFICADO DIGITAL A1 PARA PESSOA JURÍDICA
Descrição:	Essa é a solução mais antiga, os certificados são gerados e armazenados em um arquivo encriptado com acesso por senha. O usuário precisa instalar o arquivo nos ambientes onde precisar usar o certificado
Vantagens:	1. O certificado pode ser transferido para outros ambientes.
Desvantagens:	1. O arquivo pode ser facilmente copiado, ainda que precise da senha para ser descriptografado; 2. O usuário precisa saber manusear e instalar o arquivo do certificado em vários sistemas.
Análise Operacional:	Não atende
	O impacto no processo de geração e uso dos recursos de atendimento de TI é muito grande, tornando esse modelo inviável operacionalmente .

Solução PJ02 - EMISSÃO DE CERTIFICADO DIGITAL A3, COM TOKEN PESSOA JURÍDICA

Tabela 9-I

Solução:	PJ02 - EMISSÃO DE CERTIFICADO DIGITAL A3, COM TOKEN PESSOA JURÍDICA
Descrição:	O TOKEN é um dispositivo físico capaz de gerar e armazenar as chaves criptográficas que compõem os Certificados Digitais. Normalmente esse dispositivo é conectado aos computadores por meio da porta USB.
Vantagens:	- Solução mais tradicional, os usuários do Ministério estão acostumados a utilizar certificado digital com token; - Ganho em segurança com a utilização de dispositivo específico para o tratamento de certificados (token); - Vínculo dos certificados CNPJ à secretaria responsável pela escrituração e não ao CPF de um responsável; - A troca de responsáveis na secretaria não implica, necessariamente, na troca do certificado; - Não existe a necessidade de instalar aplicativos em smartphones.
Desvantagens:	- A perda do token resulta na perda do certificado; - Maior custo por certificado devido ao token.

Análise Operacional:	Atende
	Este modelo apresenta ganho significativo de segurança, devido à utilização de um dispositivo especializado para o tratamento dos certificados vinculados à secretaria, e não a uma pessoa. No entanto ele tem um custo maior, não sendo adequado para atender a um grande número de usuários.

Solução PJ03 - EMISSÃO DE CERTIFICADO DIGITAL A3, SEM TOKEN PESSOA JURÍDICA

Tabela 9-J

Solução:	PJ03 - EMISSÃO DE CERTIFICADO DIGITAL A3, SEM TOKEN PESSOA JURÍDICA
Descrição:	Essa é a solução similar à solução PF01, onde os certificados são gerados e armazenados em um arquivo encriptado com acesso por senha ou diretamente em um dispositivo token já existente. O usuário precisa instalar o arquivo nos ambientes onde precisar usar o certificado.
Vantagens:	1. O certificado pode ser transferido para outros ambientes; 2. O certificado A3 pode ser emitido com validade 36 meses, ao contrário do certificado A1; 3. O certificado pode ser gerado em um token físico já existente (token com certificado vencido).
Desvantagens:	1. Se gerado em arquivo pode ser facilmente copiado, ainda que precise da senha para ser descriptografado; 2. Se gerado em arquivo o usuário precisa saber manusear e instalar o arquivo do certificado em vários sistemas.
Análise Operacional:	Não atende
	Essa solução é similar à PJ01 e inviável operacionalmente pelos mesmos motivos já citados. No entanto ela pode ser utilizada para o processo de renovação dos tokens físicos já existentes, a um menor custo que o da solução PJ02.

Comparação das soluções para servidores - serviços

Tabela 9-K

Comparação das soluções para servidores - serviços		Soluções		
Requisitos		PJ01	PJ02	PJ03
	Garantir os requisitos de segurança da informação para os sistemas e usuários do Ministério	Atende	Atende	Atende
	Garantir a autenticidade dos documentos tramitados por servidores em cargos estratégicos do Ministério	Atende	Atende	Atende

Negócio	Garantir o atendimento à legislação vigente e ser credenciada pela Infraestrutura de Chaves Públicas Brasileira – ICPBrasil	Atende	Atende	Atende
	Garantir suporte técnico adequado para os usuários do Ministério	Atende	Atende	Atende
	A solução deverá ser implementada, preferencialmente, de forma remota	Atende	Atende	Atende
Tecnológico	A solução deve seguir padrões típicos de mercado	Atende	Atende	Atende
	A solução deve ser de fácil instalação e configuração	Não atende	Atende	Não atende
	A solução deve ser compatível com os sistemas e soluções presentes no Ministério	Atende	Atende	Atende
	A solução deve ter garantia e suporte pelo período de 36 meses	Atende	Atende	Atende
	A solução deve ser individual para cada servidor em cargos estratégicos do Ministério	não se aplica	não se aplica	não se aplica
	A solução deve garantir a proteção adequada para os níveis estratégicos do Ministério	Não atende	Atende	Não atende
Outros	A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	sim	sim	sim
	A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	não se aplica	não se aplica	não se aplica
	A Solução é composta por software livre ou software público? (quando se tratar de software)	não se aplica	não se aplica	não se aplica
	A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	não se aplica	não se aplica	não se aplica
	A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	sim	sim	sim
	A solução faz parte do Catálogo de Soluções de TIC - SISP?	não	não	não
Resultado da Análise		Não viável	Viável	Não viável

Solução SS01 - EMISSÃO DE CERTIFICADO DIGITAL A1 PARA EQUIPAMENTO SERVIDOR

Tabela 9-L

Solução:	SS01 - EMISSÃO DE CERTIFICADO DIGITAL A1 PARA EQUIPAMENTO SERVIDOR
Descrição:	Os certificados são gerados e armazenados em um arquivo encriptado com acesso por senha. O técnico responsável pelo equipamento instala o arquivo nos ambientes necessários.
Vantagens:	1. O certificado é vinculado ao domínio para o qual foi gerado; 2. O certificado pode ser transferido para outros ambientes; 3. A troca anual garante uma camada de proteção melhor ao serviço.
Desvantagens:	1. O arquivo pode ser facilmente copiado, ainda que precise da senha para ser descriptografado.
Análise Operacional:	Atende
	Solução robusta e normalmente utilizada para certificados para equipamentos servidores.

Solução SS02 - EMISSÃO DE CERTIFICADO DIGITAL A3, SEM TOKEN PARA EQUIPAMENTO SERVIDOR

Tabela 9-M

Solução:	SS02 - EMISSÃO DE CERTIFICADO DIGITAL A3, SEM TOKEN PARA EQUIPAMENTO SERVIDOR
Descrição:	Essa é a solução similar à solução SS01, onde os certificados são gerados e armazenados em um arquivo encriptado com acesso por senha ou diretamente em um dispositivo token já existente. O técnico responsável pelo equipamento instala o arquivo nos ambientes necessários.
Vantagens:	1. O certificado é vinculado ao domínio para o qual foi gerado; 2. O certificado pode ser transferido para outros ambientes; 3. O certificado A3 pode ser emitido com validade 36 meses, ao contrário do certificado A1; 4. O certificado pode ser gerado em um token físico já existente (token com certificado vencido).
Desvantagens:	1. Se gerado em arquivo pode ser facilmente copiado, ainda que precise da senha para ser descriptografado; 2. Se gerado em arquivo o usuário precisa saber manusear e instalar o arquivo do certificado em vários sistemas; 3. Para sistemas, o prazo de 36 meses acaba sendo menos indicado por questões de segurança. As normas de segurança indicam a troca anual desses certificados em ambientes mais sensíveis.
Análise Operacional:	Não atende
	Apesar da economia de custo, as normas de segurança indicam a troca anual destes certificados.

Comparação das soluções para servidores - serviços

Tabela 9-N

Comparação das soluções para servidores - serviços		Soluções	
Requisitos		SS01	SS02
Negócio	Garantir os requisitos de segurança da informação para os sistemas e usuários do Ministério	Atende	Atende
	Garantir a autenticidade dos documentos tramitados por servidores em cargos estratégicos do Ministério	Atende	Atende
	Garantir o atendimento à legislação vigente e ser credenciada pela Infraestrutura de Chaves Públicas Brasileira – ICPBrasil	Atende	Atende
	Garantir suporte técnico adequado para os usuários do Ministério	Atende	Atende
	A solução deverá ser implementada, preferencialmente, de forma remota	Atende	Atende
Tecnológico	A solução deve seguir padrões típicos de mercado	Atende	Atende
	A solução deve ser de fácil instalação e configuração	Atende	Atende
	A solução deve ser compatível com os sistemas e soluções presentes no Ministério	Atende	Atende
	A solução deve ter garantia e suporte pelo período de 36 meses	Atende	Atende
	A solução deve ser individual para cada servidor em cargos estratégicos do Ministério	não se aplica	não se aplica
	A solução deve garantir a proteção adequada para os níveis estratégicos do Ministério	Atende	Não atende
Outros	A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	sim	sim
	A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	não se aplica	não se aplica
	A Solução é composta por software livre ou software público? (quando se tratar de software)	não se aplica	não se aplica
	A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	não se aplica	não se aplica

	A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	sim	sim
	A solução faz parte do Catálogo de Soluções de TIC - SISP?	não	não
Resultado da Análise		Viável	Não viável

Soluções para certificados para servidores - domínios

Solução SD01 - EMISSÃO DE CERTIFICADO DIGITAL A1 PARA EQUIPAMENTO SERVIDOR

Tabela 9-O

Solução:	SD01 - EMISSÃO DE CERTIFICADO DIGITAL A1 PARA EQUIPAMENTO SERVIDOR
Descrição:	Os certificados são gerados e armazenados em um arquivo encriptado com acesso por senha. O técnico responsável pelo equipamento instala o arquivo nos ambientes necessários.
Vantagens:	1. O certificado é vinculado ao domínio para o qual foi gerado; 2. O certificado pode ser transferido para outros ambientes; 3. A troca anual garante uma camada de proteção melhor ao serviço.
Desvantagens:	1. O arquivo pode ser facilmente copiado, ainda que precise da senha para ser descriptografado.
Análise Operacional:	Atende
	Solução robusta e normalmente utilizada para certificados para equipamentos servidores.

Solução SD02 - EMISSÃO DE CERTIFICADO DIGITAL A3, SEM TOKEN PARA EQUIPAMENTO SERVIDOR

Tabela 9-P

Solução:	SD02 - EMISSÃO DE CERTIFICADO DIGITAL A3, SEM TOKEN PARA EQUIPAMENTO SERVIDOR
Descrição:	Essa é a solução similar à solução SS01, onde os certificados são gerados e armazenados em um arquivo encriptado com acesso por senha ou diretamente em um dispositivo token já existente. O técnico responsável pelo equipamento instala o arquivo nos ambientes necessários.
Vantagens:	1. O certificado é vinculado ao domínio para o qual foi gerado; 2. O certificado pode ser transferido para outros ambientes; 3. O certificado A3 pode ser emitido com validade 36 meses, ao contrário do certificado A1; 4. O certificado pode ser gerado em um token físico já existente (token com certificado vencido).
	1. Se gerado em arquivo pode ser facilmente copiado, ainda que precise da senha para ser descriptografado;

Desvantagens:	2. Se gerado em arquivo o usuário precisa saber manusear e instalar o arquivo do certificado em vários sistemas; 3. Para sistemas, o prazo de 36 meses acaba sendo menos indicado por questões de segurança. As normas de segurança indicam a troca anual desses certificados em ambientes mais sensíveis.
Análise Operacional:	Não atende
	Apesar da economia de custo, as normas de segurança indicam a troca anual destes certificados.

Comparação das soluções para servidores - domínios

Tabela 9-Q

Comparação das soluções para servidores - domínios		Soluções	
Requisitos		SD01	SD02
Negócio	Garantir os requisitos de segurança da informação para os sistemas e usuários do Ministério	Atende	Atende
	Garantir a autenticidade dos documentos tramitados por servidores em cargos estratégicos do Ministério	Atende	Atende
	Garantir o atendimento à legislação vigente e ser credenciada pela Infraestrutura de Chaves Públicas Brasileira – ICPBrasil	Atende	Atende
	Garantir suporte técnico adequado para os usuários do Ministério	Atende	Atende
	A solução deverá ser implementada, preferencialmente, de forma remota	Atende	Atende
Tecnológico	A solução deve seguir padrões típicos de mercado	Atende	Atende
	A solução deve ser de fácil instalação e configuração	Atende	Atende
	A solução deve ser compatível com os sistemas e soluções presentes no Ministério	Atende	Atende
	A solução deve ter garantia e suporte pelo período de 36 meses	Atende	Atende
	A solução deve ser individual para cada servidor em cargos estratégicos do Ministério	não se aplica	não se aplica
	A solução deve garantir a proteção adequada para os níveis estratégicos do Ministério	Atende	Não atende
	A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	sim	sim

Outros	A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	não se aplica	não se aplica
	A Solução é composta por software livre ou software público? (quando se tratar de software)	não se aplica	não se aplica
	A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	não se aplica	não se aplica
	A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	sim	sim
	A solução faz parte do Catálogo de Soluções de TIC - SISP?	não	não
Resultado da Análise		Viável	Não viável

10. Registro de soluções consideradas inviáveis

Soluções para certificados para pessoa física

Conforme § 1º do art. 11 da IN SGD 94/2022, as soluções identificadas e consideradas inviáveis deverão ser registradas no Estudo Técnico Preliminar da Contratação, dispensando-se a realização dos respectivos cálculos de custo total de propriedade (Total Cost Ownership – TCO).

Solução PF01 - EMISSÃO DE CERTIFICADO DIGITAL A1 PARA PESSOA FÍSICA

A Solução PF01 não é viável por não atender requisitos de operação e segurança:

O manuseio do arquivo precisa, na maioria das vezes, do apoio de um técnico;

O arquivo pode ser copiado/extraviado, o que representa um risco de segurança;

O arquivo pode ser perdido, o que causaria a necessidade da emissão de novo certificado;

A senha de acesso ao certificado pode ser perdida, o que também exige a emissão de novo certificado.

Solução PF02 - EMISSÃO DE CERTIFICADO DIGITAL MOBILE PARA PESSOA FÍSICA

Os certificados em nuvem descritos na solução PF02, são os mais utilizados hoje no Ministério. No entanto a Solução PF02 não é considerada viável porque não atende requisitos de segurança necessários a um grupo de autoridades, com cargos mais sensíveis, que atualmente utilizam o certificado com Token.

Algumas autoridades do Ministério necessitam e já utilizam a solução COM Token.

Solução PF04 - EMISSÃO DE CERTIFICADO DIGITAL A3, SEM TOKEN PESSOA FÍSICA

A Solução PF04 não é viável por não atender requisitos de operação e segurança:

O manuseio do arquivo precisa, na maioria das vezes, do apoio de um técnico;

O arquivo pode ser copiado/extraviado, o que representa um risco de segurança;

O arquivo pode ser perdido, o que causaria a necessidade da emissão de novo certificado;

A senha de acesso ao certificado pode ser perdida, o que também exige a emissão de novo certificado.

Soluções para certificados para pessoa jurídica

Solução PJ01 - EMISSÃO DE CERTIFICADO DIGITAL A1 PARA PESSOA JURÍDICA

A Solução PJ01 não é viável por não atender requisitos de operação e segurança:

O manuseio do arquivo precisa, na maioria das vezes, do apoio de um técnico;

O arquivo pode ser copiado/extraviado, o que representa um risco de segurança;

O arquivo pode ser perdido, o que causaria a necessidade da emissão de novo certificado;

A senha de acesso ao certificado pode ser perdida, o que também exige a emissão de novo certificado;

A troca do responsável exige a troca do certificado, já que o responsável anterior pode ter guardado uma cópia do arquivo.

Solução PJ03 - EMISSÃO DE CERTIFICADO DIGITAL A3, SEM TOKEN PESSOA JURÍDICA

A Solução PJ03 não é viável por não atender requisitos de operação e segurança:

O manuseio do arquivo precisa, na maioria das vezes, do apoio de um técnico;

O arquivo pode ser copiado/extraviado, o que representa um risco de segurança;

O arquivo pode ser perdido, o que causaria a necessidade da emissão de novo certificado;

A senha de acesso ao certificado pode ser perdida, o que também exige a emissão de novo certificado.

Soluções para certificados para servidores - serviços

Solução SS02 - EMISSÃO DE CERTIFICADO DIGITAL A3 PARA EQUIPAMENTO SERVIDOR

A Solução SS02 não é viável por não atender requisitos de operação e segurança:

Para sistemas, o prazo de 36 meses acaba sendo menos indicado por questões de segurança;

As normas de segurança indicam a troca anual desses certificados em ambientes mais sensíveis.

Soluções para certificados para servidores - domínios

Solução SD02 - EMISSÃO DE CERTIFICADO DIGITAL A3 PARA EQUIPAMENTO SERVIDOR

A Solução SD02 não é viável por não atender requisitos de operação e segurança:

Para sistemas, o prazo de 36 meses acaba sendo menos indicado por questões de segurança;

As normas de segurança indicam a troca anual desses certificados em ambientes mais sensíveis.

11. Análise comparativa de custos (TCO)

Registro das pesquisas no Pannel de Preços

IN Seges/ME nº 65/2021

Art. 5º A pesquisa de preços para fins de determinação do preço estimado em processo licitatório para a aquisição de bens e contratação de serviços em geral será realizada mediante a utilização dos seguintes parâmetros, empregados de forma combinada ou não:

I - composição de custos unitários menores ou iguais à mediana do item correspondente nos sistemas oficiais de governo, como Pannel de Preços ou banco de preços em saúde, observado o índice de atualização de preços correspondente;

Soluções para certificados para pessoa física

Tabela 11-A

CATSER	SEI	Quantidade de Processos	Mediana
27146	15129636	20	R\$ 153,00
27154	15129669	8	R\$ 164,50
27189	15129680	300	R\$ 195,00
27219	15129700	252	R\$ 144,50

Soluções para certificados para pessoa jurídica

Tabela 11-B

CATSER	SEI	Quantidade de Processos	Mediana
27162	15129726	64	R\$ 159,95
27197	15129753	113	R\$ 300,00
27227	15129778	41	R\$ 249,90

Soluções para certificados para servidores - serviços e domínios

Tabela 11-C

CATSER	SEI	Quantidade de Processos	Mediana
27170	15129793	25	R\$ 1.200,00

CÁLCULO DOS CUSTOS TOTAIS DE PROPRIEDADE (TCO)

Soluções para certificados para pessoa física

Custos para a Solução Viável PF03

Tabela 11-D

CATSER	Descrição	Val (m)	Qt/Ano	Val Unit	Ano 1	

27189	Cert A3 PF COM token	36	388	R\$ 195,00	R\$ 75.660,00	R\$
Custo total no ano:					R\$ 75.660,00	R\$
Custo Total de Propriedade da Solução Viável PF03:						

Custos para a Solução Viável PF05

Tabela 11-E

CATSER	Descrição	Val (m)	Qt/Ano	Val Unit	Ano 1	
27154	Cert PF em Nuvem	36	310	R\$ 164,50	R\$ 50.995,00	R\$ 5
27189	Cert A3 PF COM token	36	52	R\$ 195,00	R\$ 10.140,00	R\$ 1
27219	Cert A3 PF SEM token	36	26	R\$ 144,50	R\$ 3.757,00	R\$
Custo total no ano:					R\$ 64.892,00	R\$ €
Custo Total de Propriedade da Solução Viável PF05:						

Soluções para certificados para pessoa jurídica

Custos para a Solução Viável PJ02

Tabela 11-F

CATSER	Descrição	Val (m)	Qt/Ano	Val Unit	Ano 1	
27197	Cert A3 PJ COM token	36	18	R\$ 300,00	R\$ 5.400,00	R\$
Custo total no ano:					R\$ 5.400,00	R\$
Custo Total de Propriedade da Solução Viável PJ02:						

Soluções para certificados para servidores - serviços

Custos para a Solução Viável SS01

Tabela 11-G

CATSER	Descrição	Val (m)	Val Unit		Ano 1	
27170	Cert A1 Equip Servidor	36	R\$ 1.200,00	Qdade:	16	20

				Valor:	R\$ 19.200,00	R\$:
Custo total no ano:					R\$ 19.200,00	R\$:
Custo Total de Propriedade da Solução Viável SS01:						

Soluções para certificados para servidores - domínios

Custos para a Solução Viável SD01

Tabela 11-H

CATSER	Descrição	Val (m)	Val Unit		Ano 1	
27170	Cert A1 Equip Servidor Wildcard	36	R\$ 1.200,00	Qdade:	6	7
				Valor:	R\$ 7.200,00	F
Custo total no ano:					R\$ 7.200,00	F
Custo Total de Propriedade da Solução Viável SS01:						

MAPA COMPARATIVO DOS CÁLCULOS TOTAIS DE PROPRIEDADE (TCO)

Soluções para certificados para **pessoa física**

Tabela 11-I

	Ano 1	Ano 2	Ano 3	Total
Solução Viável PF03	R\$ 75.660,00	R\$ 75.660,00	R\$ 75.660,00	R\$ 226.980,00
Solução Viável PF05	R\$ 64.892,00	R\$ 64.892,00	R\$ 64.892,00	R\$ 194.676,00

Além de ter uma maior compatibilidade com a situação atual do Ministério, a Solução PF05 representa um ganho econômico de 14%.

Soluções para certificados para **pessoa jurídica**

Tabela 11-J

	Ano 1	Ano 2	Ano 3	Total
Solução Viável PJ02	R\$ 5.400,00	R\$ 5.400,00	R\$ 5.400,00	R\$ 16.200,00

Soluções para certificados para servidores - **serviços**

Tabela 11-K

	Ano 1	Ano 2	Ano 3	Total
Solução Viável SS01	R\$ 19.200,00	R\$ 24.000,00	R\$ 28.800,00	R\$ 72.000,00

Soluções para certificados para servidores - **domínios**

Tabela 11-L

	Ano 1	Ano 2	Ano 3	Total
Solução Viável SD01	R\$ 7.200,00	R\$ 8.400,00	R\$ 9.600,00	R\$ 25.200,00

12. Descrição da solução de TIC a ser contratada

Descrição

Contratação de Certificados Digitais A3, ICP-Brasil, para Pessoa Física, em Nuvem, com validade de 36 meses

CATSER 27154

Objetivo: Atender a demanda mensal para os cargos comissionados dos Ministérios nos próximos 36 meses

Quantidade 930 (Tabela 7-C e 9-F)

Contratação de Certificados Digitais A3, ICP-Brasil, para Pessoa Física, COM token, com validade de 36 meses

CATSER 27189

Objetivo: Atender a demanda mensal para os cargos comissionados estratégicos dos Ministérios nos próximos 36 meses

Quantidade: 156 (Tabelas 7-C e 9-F)

Contratação de Certificados Digitais A3, ICP-Brasil, para Pessoa Física, sem token, com validade de 36 meses

CATSER 27219

Objetivo: Atender a demanda mensal para os cargos comissionados estratégicos dos Ministérios nos próximos 36 meses

Quantidade: 78 (Tabelas 7-C e 9-F)

Contratação de Certificados Digitais A3, ICP-Brasil, para Pessoa Jurídica, COM token, com validade de 36 meses

CATSER 27197

Objetivo: Atender a demanda mensal para certificados de CNPJ das Secretarias dos Ministérios nos próximos 36 meses

Quantidade: 54 (Tabela 7-F)

Contratação de Certificados Digitais A1, ICP-Brasil, para Equipamentos Servidores, com validade de 12 meses

CATSER 27170

Objetivo: Atender a demanda mensal para certificados de serviços utilizados na CGI nos próximos 36 meses

Quantidade: 60 (Tabela 7-G)

Contratação de Certificados Digitais A1, ICP-Brasil, wildcard, para Equipamentos Servidores, com validade de 12 meses

CATSER 27170

Objetivo: Atender a demanda mensal para certificados de domínios utilizados na CGI nos próximos 36 meses

Quantidade: 21 (Tabela 7-G)

Justificativa

Conforme demonstrado, essa solução apresenta a melhor relação entre viabilidade técnica e custo para atender as necessidades de Certificados Digitais dos Ministérios nos próximos 36 meses, permitindo a utilização da melhor opção de segurança nos casos estratégicos e o melhor custo monetário e operacional.

13. Estimativa de custo total da contratação

Valor (R\$): 308.076,00

A Tabela 13-A sumariza a estimativa de custo total para a contratação:

Tabela 13-A - Estimativa de custo total da contratação						
Item	Descrição			Quantidade	Valor Unitário	Valor Total
	CATSER	Certificado	Val (meses)			
1	27154	Cert Pessoa Física em Nuvem	36	930	R\$ 164,50	R\$ 152.985,00
2	27189	Cert A3 Pessoa Física COM token	36	156	R\$ 195,00	R\$ 30.420,00
3	27219	Cert A3 Pessoa Física SEM token	36	78	R\$ 144,00	R\$ 11.271,00
4	27197	Cert A3 Pessoa Jurídica COM token	36	54	R\$ 300,00	R\$ 16.200,00
5	27170	Cert A1 Equip Servidor	12	60	R\$ 1.200,00	R\$ 72.000,00
6	27170	Cert A1 Equip Servidor - Wildcard	12	21	R\$ 1.200,00	R\$25.200,00
Valor Total do Contrato:						R\$ 308.076,00

14. Justificativa técnica da escolha da solução

Certificados Digitais para Pessoa Física

A solução híbrida consegue garantir todos os requisitos operacionais e de segurança esperados.

Para o grupo de usuários mais comuns a solução híbrida atende os requisitos de segurança com o melhor custo e a melhor eficiência operacional.

A necessidade de um maior grau de segurança para os usuários estratégicos é atendida com a utilização de tokens

Certificados Digitais para Pessoa Jurídica

A maior necessidade de segurança no trato dos acessos que representam os CNPJs dos Ministérios é atendida com a utilização de certificados A3 com token. Isso permite a responsabilização e o controle desses certificados dentro de cada secretaria, através do controle de acesso à mídia física do certificado.

Certificados Digitais para Serviços e Domínios

Para os serviços e domínios, a opção é a mais simples. Certificados A1 com validade de 12 meses, em acordo com o disposto nos requisitos técnicos e nas normas de segurança.

DO PARCELAMENTO DA CONTRATAÇÃO DECORRENTE DE ASPECTOS TÉCNICOS

Dado que o objeto da contratação é o "serviço de emissão de certificado digital" e os diversos itens da Tabela 13-A são apenas diferentes tipos de certificados digitais, o parcelamento da contratação não se faz necessário, porque apenas aumentaria a complexidade do processo.

15. Justificativa econômica da escolha da solução

Certificados Digitais para Pessoa Física

Serão comprados mensalmente apenas os certificados que forem efetivamente solicitados pelos Ministérios.

A solução híbrida consegue garantir a melhor economicidade ao atender a maior parte dos certificados utilizando a solução em nuvem.

Permite a possibilidade de reutilização das mídias (tokens) já existentes a um custo menor que a compra de novas mídias.

A solução não gera novos impactos na carga operacional da CGI.

Certificados Digitais para Pessoa Jurídica

Serão comprados apenas os certificados que forem efetivamente solicitados pelos Ministérios.

A solução não gera novos impactos na carga operacional da CGI.

Certificados Digitais para Serviços e Domínios

Serão comprados apenas os certificados que forem efetivamente solicitados pelos Ministérios.

A solução não gera novos impactos na carga operacional da CGI.

O PARCELAMENTO DA CONTRATAÇÃO DECORRENTE DE ASPECTOS ECONÔMICOS

Dado que o objeto da contratação é o "serviço de emissão de certificado digital" e os diversos itens da Tabela 13-A são apenas diferentes tipos de certificados digitais, o parcelamento da contratação não se faz necessário, porque apenas aumentaria a complexidade do processo.

16. Benefícios a serem alcançados com a contratação

Continuidade de diversos serviços essenciais a ambos os Ministério, entre eles:

identificação de uma autoridade em um ambiente computacional;

assinatura de documentos públicos em sistemas com, por exemplo, o SEI;

envio de informações operacionais entre órgãos públicos de forma segura;

escrituração de documentos fiscais no CNPJ do órgão ou secretaria;

manutenção de serviços públicos na internet, utilizando o protocolo HTTPS ou similar;

identificação e tráfego encriptado de dados entre sistemas de TI de órgãos distintos;

17. Providências a serem Adotadas

Não serão necessárias quaisquer providências prévias à celebração do contrato.

18. Declaração de Viabilidade

Esta equipe de planejamento declara **viável** esta contratação.

18.1. Justificativa da Viabilidade

Assim, diante do exposto ao longo dos Estudos, **entendemos ser VIÁVEL a contratação da solução demandada.**

Cenário a ser contratado

Certificados digitais para pessoa física: **Solução PF05**

Contratação de 930 Certificados Digitais A3, ICP-Brasil, para Pessoa Física, em Nuvem, com validade de 36 meses

Contratação de 156 Certificados Digitais A3, ICP-Brasil, para Pessoa Física, COM token, com validade de 36 meses

Contratação de 78 Certificados Digitais A3, ICP-Brasil, para Pessoa Física, sem token, com validade de 36 meses

Certificados digitais para pessoa jurídica: **Solução PJ02**

Contratação de 54 Certificados Digitais A3, ICP-Brasil, para Pessoa Jurídica, COM token, com validade de 36 meses

Certificados digitais para serviços disponibilizados pelo MDS: **Solução SS01**

Contratação de 60 Certificados Digitais A1, ICP-Brasil, para Equipamentos Servidores, com validade de 12 meses

Certificados digitais para domínios ssl gerenciados pelo MDS: **Solução SD01**

Contratação de 21 Certificados Digitais A1, ICP-Brasil, wildcard, para Equipamentos Servidores, com validade de 12 meses

JUSTIFICATIVA

As soluções escolhidas neste ETP, conforme todas as escolhas já detalhadas acima, permitirão a continuidade do dia-a-dia operacional e dos serviços já realizados pelo MDS e pelo MESP, atendendo os requisitos esperados de eficácia, eficiência, efetividade e economicidade:

Atende plenamente aos requisitos de negócio e aos objetivos estratégicos;

Atende aos requisitos técnicos colocados pela CGI;

Garante maior segurança aos cargos estratégicos (PF) e às secretarias (PJ);

Está em acordo com o que é atualmente utilizado nos Ministérios e não apresentará alterações operacionais;

Atende cada necessidade com o certificado mais adequado e de menor custo;

Permite o reaproveitamento das mídias (tokens) existentes que estiverem em boas condições;

Estima valores globais, mas também permite o cumprimento mensal apenas do que for efetivamente demandado.

19. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do [Decreto nº 10.543, de 13 de novembro de 2020](#).

ARTUR VICENTE SOARES DE ALBUQUERQUE

Membro da comissão de contratação

JONAS MEDEIROS LIMA

Membro da comissão de contratação



Assinou eletronicamente em 17/05/2024 às 09:42:36.